

SYSTEM AND METHOD FOR SECURELY STORING
ELECTRONIC DATA

CROSS REFERENCE TO RELATED APPLICATIONS

5 This application is related to co-pending U.S. Provisional Patent Application
Serial No. 60/081,748, entitled "Virtual Wallet System", filed April 14, 1998; co-
pending U.S. Utility Patent Application Serial No. 09/190,993, entitled "Virtual
Wallet System", filed November 12, 1998; U.S. Utility Patent Application entitled
"System and Method for Controlling Transmission of Stored Information to Internet
10 Websites," Serial No. ~~(not yet assigned)~~ ^{09/291,295} filed April 14, 1999; and, U.S. Utility Patent
Application entitled "Digital Graphic Signature System", Serial No. ~~(not yet assigned)~~ ^{09/290,427}
filed April 13, 1999; all of which are incorporated herein by reference.

FIELD OF THE INVENTION

15 This invention relates generally to storage of electronic data, and more
particularly to a system and method for securely storing, managing and updating an
owner's data and accessing the stored data by a trusted party upon the occurrence of
an event, such as the death of the owner.

20 BACKGROUND

An electronic or virtual wallet is an embodiment of software acting as a
container for electronic objects, such as payment mechanisms, identity authentication
mechanisms, personal information and electronic artifacts of the owner. The
electronic or virtual wallet can reside, for example, on one or more of a consumer's
25 personal computer (PC), a server, and a smart card. The virtual wallet allows the
owner to control access to and distribution of information in the wallet, thereby
giving the owner security and total control over the owner's personal information.
Further, the virtual wallet provides mechanisms that eliminate the risk of loss of the
information in the wallet, for example, by remotely storing and/or disabling the wallet

contents. Thus, the virtual wallet is a trusted place to keep information and valuable financial items, as well as a convenient way to move information around.

Currently, many electronic wallets focus on payment mechanisms. However, electronic wallets can also be used to maintain, for example, identification information, authentication information, certificates, access keys, personal identification numbers (PIN's), and credit card, debit card and bank account information, as well as all other types of personal information of the owner, such as the owner's will. For a detailed discussion of a virtual or electronic wallet, see, for example, currently co-pending Provisional Patent Application Serial No. 60/081,748 filed on April 14, 1998 and Utility Patent Application Serial No. 09/190,993 filed on November 12, 1998, incorporated herein by reference. Information stored in an electronic wallet can be transmitted and received by the owner of the electronic wallet, for example, through the Internet or other types of networks.

Typically, a local aspect of the virtual wallet resides on the owner's personal computer (PC) and includes a certificate or other similar authentication instrument that allows the owner to remotely gain access to the entire virtual wallet which resides, for example, on a server. The local aspect of the virtual wallet updates the remote aspect of the virtual wallet with the latest information from the local aspect when the local wallet is on-line. The server also affords greater storage capacity for the owner's information than, for example, the owner's PC. Thus, the owner is able to define and have access to all the wallet functionality at sites where the local aspect of the wallet can be linked to the server, while the remote aspect of the wallet provides security for all of the information stored in the wallet.

However, the certificate or other similar authentication mechanism, such as a special PIN, password or key that allows the owner to gain access to the owner's electronic data securely stored in the virtual wallet may typically be known only to the owner. Therefore, upon the occurrence of an event, such as the death of the owner, which makes it impossible for the owner to act, if no other person knows how to access the stored information, it may be locked up forever.

SUMMARY OF THE INVENTION

It is a feature and advantage of the present invention to provide a system and method for securely updating and managing an owner's electronic data stored in the owner's virtual wallet.

5 It is another feature and advantage of the present invention to provide a system and method for updating technologies associated with the owner's data stored in the owner's virtual wallet when such technologies become outdated.

10 It is an additional feature and advantage of the present invention to provide a system and method for accessing the owner's data stored in the owner's virtual wallet upon the occurrence of an event, such as the death of the owner.

It is a further feature and advantage of the present invention to provide a system and method for making the contents of the owner's virtual wallet available to the owner's estate upon the death of the owner.

15 To achieve the stated and other features, advantages and objects of the present invention, an embodiment of the present invention provides a system and method for securely storing, managing and updating an owner's secret data and accessing the stored data by a trusted third party upon the occurrence of an event, such as the death of the owner. An embodiment of the present invention makes use of application software, such as a virtual wallet application running, for example, at least in part on
20 the owner's personal computer and at least in part on a wallet server of a trusted third party, such as a bank or similar financial institution. The virtual wallet application also includes, for example, a virtual executor function and a virtual archivist function.

In an embodiment of the present invention, data is stored for the owner by the owner entering the data on the virtual wallet application at a terminal, such as the
25 owner's personal computer, which is coupled to the wallet server over a network, or by receiving the data from another party, such as a merchant, lawyer, or the like, for the owner, by an electronic transmission, such as an electronic mail message. The network can be a private network or a public network, such as the internet. The types of secret information entered by the owner and stored for the owner by the virtual
30 wallet application includes, for example, identification information, authentication

information, certificate information, access key information, PIN number information, credit card account information, debit card information, bank account information, and/or other personal information, such as will information, legal documents, insurance policies, brokerage account information, digital bearer instruments, digital stock certificates, and digital bond certificates.

An embodiment of the present invention involves establishing the virtual wallet for the owner for various payment functions, as well as for storing the owner's secret data. The virtual wallet application automatically assigns the owner a secret device, such as a password, secret key, PIN number, or the like, for access by the owner to the stored data, and automatically sends information about the secret device to the owner, for example, at the owner's terminal or PC coupled to the wallet server over the network. The owner's secret access device has, for example, two "flavors" or aspects, namely the owner's access aspect and the trusted third party's access aspect. The owner's access aspect is automatically sent to the owner, and the trusted third party's access aspect is automatically stored by the virtual executor function of the virtual wallet application.

In an embodiment of the present invention, the third party's access aspect of the secret device is automatically escrowed by the virtual executor function of the virtual wallet application conditioned on the occurrence of an event affecting the owner, which makes it impossible for the owner to act, such as the death or incompetence of the owner. Other secret access information is likewise automatically escrowed for the owner by the virtual executor function of the virtual wallet application, such as identification information, authentication information, certificate information, access key information, PIN number information, and password information of the owner. Likewise, various decryption infrastructure is also automatically escrowed for the owner by the virtual executor function, such as public key cryptography infrastructure, electronic document infrastructure, digital signature infrastructure, user name infrastructure, password infrastructure, fingerprint scanner infrastructure, and secret key infrastructure of the owner.

In an embodiment of the present invention, upon the occurrence of the event, such as the death or incompetence of the owner, the owner's personal representative, such as the executor or trustee of the owner's estate, presents appropriate documentation to the trusted third party necessary to verify the occurrence of the event and the representative's authority to act. Verification of the occurrence of the event is entered on the virtual executor function of the owner's virtual wallet application, and the virtual executor function automatically provides access to the owner's stored data using the escrowed information, such as the trusted third party's access aspect of the owner's secret key.

An embodiment of the present invention also includes the virtual archivist function of the owner's virtual wallet, which automatically updates the technology aspects of the stored data from time to time. The technology aspects updated by the virtual archivist include, for example, technology relating to signing a document, encryption/decryption technology, technology related to a key for signing a document, technology related to reading a document itself, technology related to translation utilities used to make the documents themselves accessible, and technology related to a certificate revocation list. Other technology aspects updated by the virtual archivist include verification and validation technology to ensure that keys, digital certificates, and notary stamps are valid as of the time stamp date associated with the documents themselves.

Additional objects, advantages, and novel features of the invention will be set forth in part in the description that follows, and in part will become more apparent to those skilled in the art upon examination of the following, or may be learned by practicing the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows schematically an overview of key components, and the flow of information between the key components, for an embodiment of the present invention;

Fig. 2 is a table which illustrates examples of the types of data which the owner stores in the owner's virtual wallet for an embodiment of the present invention;

Fig. 3 is a table which shows examples of the types of information escrowed by the virtual executor for an embodiment of the present invention;

Fig. 4 is a table which shows examples of the two "flavors" for the key for accessing the owner's virtual wallet for an embodiment of the present invention;

5 Fig. 5 is a flow chart which amplifies the flow of information shown in Fig. 1 and provides further detail regarding the process of escrowing and accessing the owner's stored data for an embodiment of the present invention; and

Fig. 6 is a table which shows examples of the types of technologies which are updated by the virtual archivist for an embodiment of the present invention.

10 DETAILED DESCRIPTION

Referring now in detail to an embodiment of the present invention, an example of which is illustrated in the accompanying drawings, the present invention provides a system and method for securely storing, updating and managing an owner's electronic data and accessing the stored data by a trusted third party upon the occurrence of an event, such as the death or incompetence of the owner. Fig. 1 shows schematically an overview of key components, and the flow of information between the key components, for an embodiment of the present invention. The system for an embodiment of the present invention makes use of application software, such as a virtual wallet, which resides, for example, on one or both of the PC 2 of the owner 4 and a server 6 of a financial institution 8, such as a bank.

Fig. 2 is a table which illustrates examples of the types of data which the owner stores in the owner's virtual wallet for an embodiment of the present invention. Referring to Figs. 1 and 2, a local aspect 10 of the virtual wallet 12 residing on the owner's PC 2 allows the owner 4 to remotely gain access to the entire virtual wallet 14, which resides on the wallet server 6, over a network 16, such as the Internet. The local aspect 10 updates the remote aspect 14 of the virtual wallet 12 with the latest information from the local aspect when the local wallet is on-line to the server 6. Types of information which may be stored for the owner 4 in the virtual wallet 12 include, for example, identification information 18, authentication information 20,

certificates 22, access keys 24, personal identification numbers (PIN's) 26, credit card account information 28, debit card information 30, bank account information 32, and other personal information 34, such as the owner's will, legal documents, insurance policies, brokerage account information, digital bearer instruments, digital stock certificates, and digital bond certificates.

Referring further to Fig. 1, a certificate or other similar authentication mechanism 36, such as a special PIN, password, or key, typically known only to the owner 4, allows the owner to gain access to the owner's electronic data securely stored in the virtual wallet 12. Generally, all of the digital services that are related to electronic commerce, such as public key cryptography, electronic documents, and digital signatures, rely on the person who holds the certificate or who owns the wallet being present to access them. It can be as simple, for example, as a user name and password, if the owner 4 actually keeps the owner's password private. On the other hand, it can be as complicated as a fingerprint scanner requiring a live thumbprint that has, for example, a body temperature. When the owner 4 dies, access to the owner's decryption infrastructure is likewise gone, and the access, in effect, dies with the owner.

A functionality within the virtual wallet for an embodiment of the present invention provides a solution to the problem by maintaining a file with all of this critical information that can be opened by a trusted third party, such as the financial institution 8, e.g., a bank, upon the death of the owner 4. This allows for the settlement of all accounts and for access to information by the successors in interest of the owner 4. Referring again to Fig. 1, this aspect of an embodiment of the present invention, referred to as the virtual executor 38, allows access to the owner's secure electronic data stored in the electronic wallet 12 once the owner 4 is, for example, deceased or legally incompetent or otherwise incapable of conducting her own affairs. Thus, the virtual executor 38 provides for the owner's secure information to be passed on to the owner's successors in interest after the owner 4 is, for example, deceased, incompetent, or otherwise unable to act on the owner's own behalf.

The virtual executor 38 functionality for an embodiment of the present invention provides a service that escrows the keys and/or similar access devices or mechanisms, so that when the owner 4 dies, the keys become part of the owner's estate and can be handled as part of the typical estate settlement. Fig. 3 is a table which shows examples of the types of information escrowed by the virtual executor 38 for an embodiment of the present invention. The types of information escrowed by the virtual executor 38 include, for example, identification information 18, authentication information 20, certificates, 22, access keys 24, PIN numbers 26, passwords 40, and other similar secret access mechanisms 42. Without the virtual executor 38, all of the owner's information that is protected, for example, by authentication information 20, keys 24, special PIN's 26, or passwords 40 may be forever locked up with the unavailability of the owner 4 to act, who is typically the only one who knows how to access the information stored in the virtual wallet 12.

In an embodiment of the present invention, the owner's secret keys and/or other similar access devices are escrowed with the trusted third party which is, for example, the financial institution or bank 8, through the virtual executor 38, which is a type of virtual trust for the owner 4. The owner 4 escrows the owner's secret keys with the trusted third party 8, and the escrowed keys become part of the owner's estate. In other words, the escrowed keys are similar to the owner's will and all the other trusts that the owner 4 may have. For example, the owner 4 can also have electronic funds, such as stored value or digital coins, that require the owner's thumbprint to decrypt. Upon the occurrence of an event, such as the death or incompetence of the owner, the system and method for an embodiment of the present invention provides a way for the trusted third party 8 to obtain access to the value that is stored, for example, in those coins.

The system and method for an embodiment of the present invention provides, for example, a technology infrastructure associated with the virtual wallet 12 for accessing the contents of the virtual wallet, such as the owner's stored value in the wallet. The technology infrastructure associated with the virtual wallet 12 provides a key that is durable and has, for example, two "flavors." Fig. 4 is a table which shows

examples of the two "flavors" for the key 44 for accessing the owner's virtual wallet 12 for an embodiment of the present invention. A first flavor of the key is the owner's secret access mechanism 36, which is necessary for the owner 4 to use every day for access to the virtual wallet 12. A second flavor 46 of the key is held by the trusted third party 8 to give the third party access to the virtual wallet 12. The second flavor 46 is, in effect, like a master key that gives the trusted third party 8 access to the contents of the owner's virtual wallet 12 once the owner 4 is no longer able to use the owner's primary access device 36.

Fig. 5 is a flow chart which amplifies the flow of information shown in Fig. 1 and provides further detail regarding the process of escrowing and accessing the owner's stored data for an embodiment of the present invention. At S1, the owner 4 at a terminal, such as the owner's PC 2, establishes the virtual wallet 12. At S2, the owner automatically receives a new key 36 that gives the owner access to the wallet. At S3, starting with that key 36, a key escrow is automatically created with the trusted third party 8 by the virtual executor functionality 38 within the virtual wallet 12. The virtual executor functionality 38 automatically assures that the key 36 is appropriately escrowed. When an event occurs, such as the death of the owner 4, the owner's personal representative presents the appropriate notice about the owner's death, such as a death certificate, to the trusted third party 8 at S4, and the virtual executor 38 is assured that the owner is actually deceased. At S5, the virtual executor 38 uses its set of keys to make available to the estate all of the content that the owner 4 has protected by those keys. For example, if it is the owner's access to digital funds within the owner's virtual wallet 12, one of those keys will allow access to those funds.

In an embodiment of the present invention, in addition to secret keys, the owner 4 may also have various other information stored in the virtual wallet 12, such as the owner's will 34. The owner 4 may have stored, for example, an electronic copy of the owner's will 34 in the data archive associated with the owner's virtual wallet 12 as the official copy of the will. Referring again to Fig. 5, at the death of the owner 4, the owner's personal representative takes a copy of the appropriate death certificate and/or other appropriate documentation to prove the authority of the personal

representative and physically presents the documentation to the trusted third party 8. When the virtual executor 38 is assured of the owner's death, the virtual executor likewise uses its set of keys to make the owner's stored will 34 available to the owner's estate at S5. Demonstrating and documenting the owner's death, as well as the authority of the owner's personal representative to act upon the owner's death, to the trusted third party 8 is a part of the security mechanism for an embodiment of the present invention.

A further aspect for an embodiment of the present invention is a functionality within the virtual wallet 12, referred to as the virtual archivist, which provides for access and updating of the electronic information stored in the virtual wallet, for example, when various technologies associated with the stored information become outdated. Fig. 6 is a table which shows examples of the types of technologies which are updated by the virtual archivist for an embodiment of the present invention. The virtual archivist 46 updates technologies, such as those used to sign documents 48, encrypt/decrypt documents 50, keys 52, read the documents themselves 54, file translation utilities used to make the documents themselves accessible 55, and certificate revocation lists 56, to conform to changes in technology. The virtual archivist 46 also updates verification and validation technologies to ensure that keys 52, digital certificates 57, and notary stamps 60 are valid as of the time stamp date 58 associated with the documents themselves. Further, in an embodiment of the present invention, the virtual archivist 46 takes the information with the outdated technology and updates it to make it compatible with the latest technology, while maintaining the integrity of the original information. Thus, the virtual archivist 46 enables all information to conform to the latest technological advances.

For example, as electronic documents become, in effect, the original documents, the owner's will 34 stored electronically in the data archive part of the owner's virtual wallet 12 becomes the owner's official will. The owner's will written today may be written in an application, such as Word 7.0, which runs on an Intel Pentium computer with an operating system, such as Windows NT 4.0. If the owner dies at a much later time in the future, it may be unlikely that a copy of Word 7.0, or

an Intel computer, or a copy of NT 4.0 will be readily available. Therefore, when the owner 4 dies in the future, in spite of the fact that the owner's will was signed and encrypted and protected and the owner has stored and archived all the keys so that the virtual executor has access to them, it may still not be possible to read the file because the access mechanisms have ceased to exist.

In an embodiment of the present invention, the virtual archivist 46 is, in effect, a responsibility functionality. As the owner's files are archived in the data archive associated with the owner's virtual wallet 12, the virtual archivist 46 maintains the stored files in a way that the files can be accessed over time by automatically updating the stored data and the technologies associated with the data as the technologies change over time. The virtual archivist 46 is part of one of the functionalities within the virtual wallet 12 that is the personal information archive. As the owner 4 inputs the owner's data into the data archive associated with the virtual wallet 12, the virtual archivist 46 is automatically informed of what the owner's data is and automatically formats the data, so the data can continue to be useful.

Various preferred embodiments of the invention have been described in fulfillment of the various objects of the invention. It should be recognized that these embodiments are illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be readily apparent to those skilled in the art without departing from the spirit and scope of the present invention. Accordingly, the invention is limited only by the following claims.